

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri**FILED**MAR 10 2021U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUISIn the Matter of the Search of
THE PREMISES LOCATED AT:
249 Mount Everest Drive, Apartment C
Fenton, Missouri 63026) 4:21 MJ 5067 NAB
) **FILED UNDER SEAL**
) SIGNED AND SUBMITTED TO THE COURT FOR
) FILING BY RELIABLE ELECTRONIC MEANS
)
)**APPLICATION FOR A SEARCH WARRANT**I, BRIAN MEADOWS, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:**See Attachment A**located in the Eastern District of Missouri, there is now concealed**See Attachment B**The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- xx evidence of a crime;
- xx contraband, fruits of crime, or other items illegally possessed;
- xx property designed for use, intended for use, or used in committing a crime;
- xx a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section**Offense Description*

Title Section

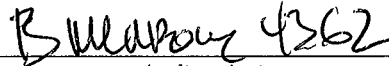
18 U.S.C. §2422 (coercion and enticement of a minor), 18 U.S.C. 2251 (attempted production of child pornography) and 18 U.S.C. 2252A (attempted receipt and possession of child pornography)

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

*Applicant's signature*

Brian Meadows, TFO, FBI

Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: 03/10/2021*Judge's signature*City and State: St. Louis, MOHonorable Nannette A. Baker, U.S. Magistrate Judge*Printed name and title*

AUSA: Jillian Anderson

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF)	
THE PREMISIS LOCATED WITHIN THE)	No. 4:21 MJ 5067 NAB
EASTERN DISTRICT OF MISSOURI AT:)	
249 Mount Everest Drive, Apartment C)	
Fenton, Missouri 63026)	FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Brian Meadows, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 249 Mount Everest Drive, Apartment C, Fenton, Missouri 63026 (hereinafter the “Premises”) further described in Attachment A, for the things described in Attachment B.

2. I am a Task Force Officer with the Federal Bureau of Investigation and have been since July of 2019. I am a detective with the St. Louis County Police Department (SLCPD), duly appointed according to law and acting as such. I have been employed with the SLCPD for approximately six (6) years, and have been in my current assignment as a Criminal Intelligence detective for approximately two years. Prior to my current assignment I was assigned to the SLCPD Special Response Unit for approximately one year. I have been and currently am a deputized federal task force officer with the Federal Bureau of Investigation and am assigned to the Violent Gang Safe Streets Task Force. During my time as a law enforcement officer, I have utilized a variety of investigative techniques to include: organizing and participating in physical surveillance; participating in undercover operations; serving search warrants; making arrests; and

interviews involving defendants. In connection with my official duties, I have investigated and currently investigate criminal violations of state and federal laws. I have participated in numerous complex investigations of individuals and violent crime organizations dealing in robberies, carjackings, homicides, assaults, weapons violations, sex offenses, and other criminal violations of state and federal laws. I have participated in numerous investigations that have resulted in the identification, apprehension, prosecution, and conviction of violent and non-violent criminal actors.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other officers, agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §2422 (coercion and enticement of a minor), 18 U.S.C. 2251 (attempted production of child pornography) and 18 U.S.C. 2252A (attempted receipt and possession of child pornography) have been committed by Robert L. Payne. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

LOCATION TO BE SEARCHED

5. The location to be searched is:

249 Mount Everest Drive, Apartment C, Fenton, MO 63026, the Premises is described as Attachment A.

TECHNICAL TERMS AND DEFINITIONS

6. Based on my training and experience and discussions I have had with other law enforcement officials, I use the following terms to convey the following meanings:

a. “Digital device,” as used herein, includes the following terms and their respective definitions:

i) A “computer” means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

ii) “Digital storage media,” as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks (“DVDs”), USB flash drives, flash memory cards, and internal and external hard drives.

iii) “Computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

iv) “Wireless telephone” (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through “wi-fi” networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional “land line” telephones, computers, and other digital devices. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files;

storing dates, appointments, and other information on personal calendars; utilizing global positioning system (“GPS”) locating and tracking technology, and accessing and downloading information from the Internet.

v) A “tablet” is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, “wi-fi” networks, or otherwise. Tablets typically contain programs called applications (“apps”), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

vi) A “GPS” navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated “GPS”) to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

b. “Computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data. Data

security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. Cloud storage,” as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user’s computer or other local storage device) and is made available to users over a network, typically the Internet.

e. A “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

f. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

g. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

h. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

i. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

j. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation;

(d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

k. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

PROBABLE CAUSE

7. I and/or other law enforcement officers in the Criminal Intelligence Unit of the SLCPD, as part of ongoing investigations into Child Enticement offenses, came across the following suspect, ROBERT L. PAYNE (White Male, DOB: 05/06/1945, Social Security Number ending in 2218) of 249 Mount Everest Drive, Apt. C, Fenton, Missouri 63026.

8. After receiving several citizen complaints and conducting numerous hours of surveillance at Fenton City Park, located at 1215 Larkin Williams Road, and observing Payne’s repeated attempts to contact male minors, on March 8, 2021, Detectives placed an undercover male minor (“Tyler”), portrayed by a St. Louis County Police Officer bearing a youthful appearance and small stature, in the basketball courts adjacent to Payne, who remained stationary in his red 2003 Ford Ranger.

9. After approximately 30 minutes of playing basketball, “Tyler” proceeded to a trashcan near Payne’s truck, to throw away an empty Gatorade bottle, and was engaged in conversation by Payne, which was audio-captured by a covert body-worn device. Payne

informed “Tyler” that he watched him ride his bike to the basketball courts and that he was a “good looking kid”, before asking “Tyler” how old he was. “Tyler” stated “16”, to which Payne replied, “16! ...That’s jail-bait!” Payne made reference to “Tyler’s” legs being pale white, and later stated that he would “Not want anything in return, but would like to suck his (“Tyler’s”) dick sometime”.

10. Payne asked “Tyler” to exchange numbers to meet at a later date, at which point he provided “Tyler” with a home telephone number, a cellular telephone number, and an email address of RPayne2@PeoplePC.com. “Tyler” provided Payne with undercover email account TylerW7404@Gmail.com. Payne invited “Tyler” to sit in his truck and watch the basketball game and he would “play with his (“Tyler’s”) dick a little bit”. “Tyler” declined the offer and left the area. Prior to departing, Payne stated, “I’d like to play with that dick a little sometime”. Detectives left the area at approximately 4PM on March 8th.

11. At approximately 6:35PM on March 8th, Detective Meadows received an email to undercover account TylerW7404@Gmail.com from RPayne2@PeoplePC.com, with the subject “White Legs”, and engaged in the following conversation:

RPayne2: “Wanted to see if I had right email”

TylerW7404: “White legs lol. Is this Bob from the park?”

RPayne2: “yes only thing wrong with ur legs is my head is not between them”

TylerW4704: “Oh wow lol!”

As the conversation progressed, RPayne2@PeoplePC.com proceeded to make the following

statements:

“safest place is my apt no cops here”

“I would not do anything to hurt u and told u I want no return at all ///// lay u on my bed and suk all the juice out of u”

“only wanna suk u off and become friends let me cum pick u up //// are u back in school 5 days a week”

“wanna suk ur dic // do u have a curfew”

“I wanna suk all the cum outta ur dic and swallow it /// I wil b at park tomorrow same lot at 11 am and 3pm cum cum to me”

“see u tomorrow at park 3pm /// u can get in and I can at least get it hard //// if u need me to pic u up near ur home just tell me”

“I will wait don’t hurry don’t get hurt /// don’t bruise ur dic r skin up ur white legs //// luv u already”

“u could send me pics of it soft r hard and I wil hav something to lick on”

Tyler7404 then asked, “Is your email on phone or computer?” to which Rpayne2 replied, “Computer”. RPayne2 ended the conversation a short time later with, “suk suk suk”.

12. Payne listed his current address on his Missouri issued driver license as 249 Mount Everest Drive Apartment C, which is the same address indicated on the registration of his red 2003 Ford Ranger. On numerous prior occasions, Detectives observed Payne’s red Ford Ranger parked in front of the building located at 249 Mount Everest Drive.

13. Surveillance revealed that Robert Payne parked at the Fenton City park each day between March 1, 2021 and March 4, 2021. Payne was seen parked near the Basketball courts on March 1st. Over the course of March 2nd and 3rd, Payne was observed to be at the Fenton City park from about 3:30 p.m. to 6:30 p.m. each day. On March 2nd, he was observed to reposition his vehicle within the Fenton City park about eighteen times, including backing into a space to allow his view of the Lindbergh High School boys lacrosse team practice. On March 3rd, Payne was observed to attempt to engage about ten to twelve young males in the area of the basketball courts at Fenton City park.

14. On March 4th, Detective Meadows applied to the 21st Judicial Circuit Court of the State of Missouri and obtained a search warrant to place a GPS tracking device on Payne's red Ford Ranger, based upon a prior active Sexual Misconduct investigation, which occurred in Fenton City Park. That investigation stemmed from a report that on the afternoon of February 5th, 2021, a 17-year old male victim was playing basketball at Fenton City Park when he was approached by a suspect, who was later identified as Robert Payne. During a brief conversation, victim was asked his age, to which he replied "17". Several minutes later Payne asked the victim to exchange numbers and meet up at a later date "for sex". Since placement of the device on March 5th, investigators have observed Payne's vehicle to travel to the area of 249 Mount Everest Drive around 6:30 p.m. every evening and remain until the following morning.

15. A review of reports from various law enforcement agencies reveals that Robert Payne has a pattern of targeting minors for sexual contact:

- Velda City Police Report #13-52 indicates that Robert Payne responded to a Craigslist advertisement in January 2013, utilizing the email address RPayne2@PeoplePC.com, and communicated with what he believed to be a 15 year old boy for approximately 25 days. Throughout the duration of the conversations, Payne repeatedly told the decoy that he wanted to perform oral sex on him and continuously attempted to arrange a meeting. Payne was arrested after a pre-planned meeting was arranged with the decoy, at which time two firearms were recovered from Payne's vehicle. No charges were issued as a result of this investigation.

- Sunset Hills Police Department report #18-10916 indicates that Robert Payne was parked in his red Ford Ranger at Mini HaHa park in Sunset Hills, when he approached a 16 year old male, and asked if he could take him back to his apartment and perform oral sex on him. Payne was arrested in possession of a pistol and was initially charged with state level Sexual Misconduct 2nd and attempted Statutory Sodomy 2nd, but eventually pled guilty to Harassment.

- Jefferson County Sheriff's Office report #19-28569 indicates that Robert Payne got into an altercation with his adult male neighbor and was eventually arrested in possession of a pistol and charged with Assault 4th Degree. Adult male neighbor stated that he confronted Payne after he witnessed him making sexual advances toward his minor son and attempted to exchange phone numbers with him. Payne admitted he attempted to exchange phone numbers with the minor, but stated that it was not for sexual purposes. Payne stated that he retrieved his firearm after he was confronted and stated he would, "blow his (adult neighbor) fucking brains out" if he came on Payne's lawn.

16. Based on the foregoing, I believe there is probable cause to conclude that Robert L Payne has violated 18 U.S.C. §2422 (coercion and enticement of a minor), 18 U.S.C. 2251 (attempted production of child pornography) and 18 U.S.C. 2252A (attempted receipt and possession of child pornography).

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO ARE INTERESTED IN
CHILD PORNOGRAPHY AND CHILD SEXUAL EXPLOITATION**

17. Based on my previous investigative experience and the training and experience of other law enforcement officers with whom I have worked had discussions, I know there are certain characteristics common to individuals who utilize the internet, digital communications and digital devices to sexually exploit children:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals may possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to solicit, produce, and share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers

of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

18. Based on all of the information contained herein, I believe that the user of the Subject Devices, Robert Payne, likely displays characteristics common to individuals who access online child sexual abuse and exploitation material. For example: Robert Payne utilized one or more digital devices to solicit sexually explicit images of “Tyler” that would be easily stored and transferred via electronic and internet-based means.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

19. Based on my knowledge, training, and experience, as well as information related to me by investigators and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are found on the Premises, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, including violation of 18 U.S.C. §2422 (coercion and enticement of a minor), 18 U.S.C. 2251 (attempted production of child pornography) and 18 U.S.C. 2252A (attempted receipt and possession of child pornography), utilize text

messaging, social media, other means of cellular telephone and online communication, and electronic devices capable of accessing the internet to meet children, to communicate with children regarding details relevant to criminal activity, locate children using GPS technology and to receive and distribute images and/or videos relevant to criminal activity and communication with children.

b. The investigation has revealed that Payne utilized computer, wireless telephone, internet and cellular technology to communicate with “Tyler” and attempt to arrange meetings for the purpose of engaging in illicit sexual contact, to solicit the production and dissemination of child pornography and to exchange other information with “Tyler” in a manner that facilitated his criminal activity with “Tyler.” Such internet and cellular technology is stored, downloaded and accessed via wireless telephones and digital devices.

c. Computers and digital technology are the primary way in which individuals interested in child pornography and illicit sexual contact with minors interact with each other and with minors. Computers basically serve five functions in connection with child pornography: solicitation, production, communication, distribution, and storage.

d. Based on my experience and training and that of other law enforcement officers with whom I have worked, individuals who engage in unlawful sexual activity and unlawful sexual activity involving children often videotape or otherwise record and maintain such unlawful activity utilizing cameras or other digital recording devices as well as digital storage devices on which such recordings and videos can be maintained and stored.

e. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

f. Mobile devices such as smartphones and tablet computers may connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) solicited, produced, distributed, and received by anyone with access to a computer or smartphone.

g. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual’s person. Smartphones and/or mobile phones are also often carried on an individual’s person.

h. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

i. Individuals also use online resources to solicit, produce, retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer, smartphone, or external media in most cases.

j. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as “apps.” Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

k. Individuals who engage in the foregoing criminal activity utilizing wireless telephones and digital devices will often utilize more than one such telephone or device, change wireless telephones and digital devices, and will often “back up” or transfer files from their old wireless telephones and digital devices to their new wireless telephones or digital devices, so as

not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

l. Based on my training and experience I know that electronic devices and mobile phones (a) are capable of being used to send and receive text messages, photographs, short videos, other electronic data and voice communication; (b) contain an internal memory which can store records of received, dialed, and missed calls or messages and can store data downloaded from the internet, pictures, text messages, phone books, address books, and other data; (c) often contain personal information to identify the owner of that particular phone and can also store the last number dialed, along with information about the geographical location of the cellular tower that was used to place phone calls; (d) are often equipped with Subscriber Identity Module (SIM) cards. A SIM card is a removable chip inside a cellular phone and/or personal digital assistant device that contains information such as the user's phone number, phone book as well as other information related to the subscriber.

m. Based on my training and experience, as well as discussions I have had with other trained agents and investigators, I know that mobile telephones contain a variety of stored electronic data. For example, mobile phones maintain call logs that record the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, mobile telephones often referred to as “smart phones” offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still

photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

n. As is the case with most digital technology, communications by way of computer, mobile phone, tablet, or other similar electronic media can be saved or stored on the device. Storing such information can be intentional, i.e., by saving an e-mail as a file on a computer or tablet, or saving the location of one's favorite websites such as "bookmarked" or “favorite” files. Digital information can also be retained unintentionally, such as traces of the path of an electronic communication that may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). Applications operating on electronic devices also store data about the device user, times and locations of when an application may be operated by the user, and other data related to the general use of the application (such as a photo, a message, a search, etc.)

o. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person

“deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

p. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

q. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

r. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

s. As further described in Attachment B, this application seeks permission to locate not only data that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how wireless telephones and/or digital devices were used, the purpose of their use, who used them, and when. There is probable cause to believe

that this forensic electronic and digital evidence will be on any storage medium in the Premises because:

t. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

u. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate

who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the

offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

v. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

w. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

x. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

20. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

21. In most cases, a thorough search of a premises for information that might be stored on a digital device often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the digital devices to obtain evidence. Digital devices can store a large volume

of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

22. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

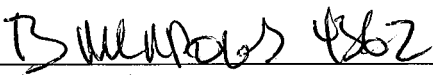
CONCLUSION

23. Based on the foregoing I submit that this affidavit supports probable cause for a warrant to search the Premises described in Attachment A and seize the items described in Attachment B.

24. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.


I state under the penalty of perjury that the foregoing is true and correct.

Respectfully submitted,



Brian Meadows
Federal Task Force Officer
Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41, on March 10, 2021.



The Honorable Nannette A. Baker
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is 249 Mount Everest Drive, Apartment C, Fenton, Missouri 63026 further described as an interior dwelling located within the following image of the apartment building at 249 Mount Everest Drive, inside which Apartment C is located:



ATTACHMENT B

Property to be seized and searched

1. All items, data, records and information relating to violations of 18 U.S.C. §2422 (coercion and enticement of a minor), 18 U.S.C. 2251 (attempted production of child pornography) and 18 U.S.C. 2252A (attempted receipt and possession of child pornography) that constitutes fruits, evidence and instrumentalities of such violations those violations involving Robert L. Payne, including:

- a. Photographs of the exterior and interior of the residence at 249 Mount Everest Drive, Apartment C, Fenton, Missouri 63026, and
- b. Wireless telephones, computers, digital devices, electronic devices and data storage devices (hereinafter collectively referred to as “Device(s)”).

2. For any Device(s) whose seizure is otherwise authorized by this warrant, and any Device(s) that contain or in which records or information are stored that is otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence

of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the Device(s) were accessed or used to determine the chronological context of the Device(s) access, use, and events relating to crime under investigation and to the Device(s) user;
- e. evidence indicating the Device(s) user's state of mind as it relates to the crimes under investigation and relevant to child pornography or any visual depictions of minor females and males posed in sexually explicit positions or engaging in sexually explicit conduct or attempted grooming, enticement or coercion of a minor to engage in sexual conduct;
- f. evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);
- h. evidence of the times the Device(s) were used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the Device(s);
- j. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);
- k. records of or information about Internet Protocol addresses used by the Device(s);

- l. records of or information about the Device(s) Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment;
- n. evidence of communications with minors or attempts to communicate with minors for the purpose of engaging in illicit sexual activity with such minors; possessing, receiving or producing obscene or sexual material involving minors, or the grooming of minors for such ends;
- o. images, photographs, videos and other material depicting minors or simulated minors engaged in sexual acts, the lascivious display of their genitals or erotic material depicting actual or simulated minors;
- p. All data files, including but not limited to graphic representations, containing matter pertaining to child pornography, that is, visual depictions of minors posed in sexually-explicit positions or engaging in sexually-explicit conduct and communications pertaining to grooming, enticing or coercing minors to engage in sexual conduct;
- q. Graphic interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI and MPEG) containing matter pertaining to child pornography or attempted grooming, enticement or coercion of a minor to engage in sexual conduct;

- r. Electronic mail, chat logs, and electronic messages, offering to transmit or soliciting through interstate or foreign commerce, including by United States mail or by computer, visual depictions of minors posed in sexually explicit positions or engaging in sexually explicit conduct or attempted grooming, enticement or coercion of a minor to engage in sexual conduct;
- s. All correspondence and communications regarding the solicitation, possession, distribution, sale or receipt child pornography or attempted grooming, persuasion, inducement, enticement or coercion of a minor to engage in sexual conduct;
- t. Any and all correspondence identifying persons transmitting, through interstate commerce including by computer/email/internet/social media, any information related to child pornography or any visual depictions of minors posed in sexually explicit positions or engaging in sexually explicit conduct or attempted grooming, enticement or coercion of a minor to engage in sexual conduct;
- u. Any and all records, data and ledgers bearing on the solicitation, production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission, through interstate commerce including by United States Mails or by computer, any information related child pornography or any visual depictions of minors posed in sexually explicit positions or engaging in sexually explicit conduct or attempted grooming, enticement or coercion of a minor to engage in sexual conduct; and

- v. Data that shows the physical location or route of travel of the user of the device relevant to attempted grooming, enticement or coercion of a minor to engage in sexual conduct.

3. As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

4. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied

electronic data to the custody and control of attorneys for the government and their support staff for their independent review.